PARA ALÉM DA PROTEÇÃO DE DADOS: **UMA COLETÂNEA**

AUTORES

Anna Bentes
Bruno Bioni
Paula Guedes
Pedro H. Santos
Pedro Martins
Sinuhe Cruz

EDITORA
DATA PRIVACY BRASIL

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Para além da proteção de dados [livro eletrônico] : uma coletânea / Anna Bentes... [et al.]. -- São Paulo : Data Privacy Brasil Ensino, 2023. PDF

Outros autores: Bruno Bioni, Paula Guedes, Pedro H. Santos, Pedro Martins, Sinuhe Cruz.
Bibliografia.
ISBN 978-65-85344-00-5

1. Direito e tecnologia 2. Direito - Coletâneas 3. Proteção de dados - Direito - Brasil 4. Proteção de dados - Leis e legislação I. Bentes, Anna. II. Bioni, Bruno. III. Guedes, Paula. IV. Santos, Pedro H. V. Martins, Pedro. VI. Cruz, Sinuhe.

23-146358 CDU-34:6

Índices para catálogo sistemático:

1. Direito e tecnologia 34:6

Eliete Marques da Silva - Bibliotecária - CRB-8/9380

Organizadores
Anna Bentes
Paula Guedes
Pedro Martins
Pedro Henrique Santos
Bruno Bioni

Autores
Anna Bentes
Bruno Bioni
Paula Guedes
Pedro Martins
Pedro Henrique Santos
Sinuhe Cruz

Revisor
Sinuhe Cruz

Time de apoio
Gedeão França

Design
Roberto Junior

Sobre os autores

ANNA BENTES

Anna Bentes é Professora Adjunta na Escola de Comunicação, Mídia e Informação da Fundação Getúlio Vargas (ECMI-FGV). É Doutora e mestre em Comunicação e Cultura pela Universidade Federal do Rio de Janeiro (UFRJ) e formada em Psicologia pela UFRJ. É autora do livro "Quase um tique: economia da atenção, vigilância e espetáculo em uma rede social'', pela editora UFRJ (2021), e Membro do Conselho Diretivo da Rede Latino Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (LAVITS). É colunista do Terra Byte, onde fala sobre temas relacionados à tecnologia e comportamento. Atualmente, é *Fellow* da Derechos Digitales, liderando uma pesquisa sobre desinformação nas eleições brasileiras de 2022. Em suas pesquisas, está interessada na intersecção entre Comunicação, Psicologia e Mídias Digitais.

BRUNO BIONI

Doutor em Direito Comercial e Mestre em Direito Civil na Faculdade de Direito da Universidade de São Paulo - USP. Membro do Conselho Nacional da Autoridade Nacional de Proteção de Dados - CNPD, designado como titular dentre os representantes de organizações da sociedade civil. Foi *study visitor* do Departamento de Proteção de Dados Pessoais do *European Data Protection Board* - EDPB e do Conselho da Europa-CoE, pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa. É autor do livro "Proteção de Dados Pessoais: a função e os limites do consentimento'' e co-autor do livro "Proteção de dados: contexto, narrativa e elementos fundantes". É membro da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade - LAVITS. É diretor fundador do Data Privacy Brasil, um espaço de intersecção entre uma escola de cursos e uma associação de pesquisa na área de privacidade e proteção de dados. É advogado, consultor e parecerista.

PAULA GUEDES

Doutoranda em Direito pela Universidade Católica Portuguesa – Centro Regional do Porto (bolsista da Fundação para a Ciência e Tecnologia) e Mestre em Direito Internacional e Europeu pela mesma instituição; especialista em Direito Digital pelo ITS-Rio em parceria com a UERJ. Pesquisadora do grupo de pesquisa em Direito e Tecnologia da PUC-Rio (Legalite) e membro do Grupo de Estudos em Novas Regulações de Serviços Digitais no Direito Comparado do *Legal Grounds Institute*.

PEDRO HENRIQUE SANTOS

Graduado em Direito pela Universidade Federal de Juiz de Fora. Advogado e colaborador externo do Centro de Referência em Direitos Humanos da Universidade Federal de Juiz de Fora - Campus Governador Valadares. É membro do setor acadêmico do Data Privacy Brasil Ensino.

PEDRO MARTINS

Mestre em Direito pela Universidade Federal de Minas Gerais. Desenvolve pesquisa na área de proteção de dados pessoais e profiling. É autor do livro “Profiling na Lei Geral de Proteção de Dados: O livre desenvolvimento da personalidade em face da governamentalidade algorítmica” pela editora Foco (2022). Pesquisador do grupo de pesquisa Persona e Coordenador Acadêmico do Data Privacy Brasil.

SINUHE CRUZ

Bacharel em Direito pela Universidade de São Paulo e pesquisador nas áreas de privacidade, proteção de dados e regulação de novas tecnologias. Colaborou como Analista Acadêmico do Data Privacy Brasil entre 2020 e 2022

Sumário

INTRODUÇÃO 07

PARTE I - Introduzindo a LGPD 12
1. Linha do tempo da Proteção de Dados no Brasil: 2 anos da LGPD em vigor 13
2. Dado pessoal: um conceito em disputa 28
3. Descomplicando a LGPD: Como escolher a base legal adequada 33
4. Descomplicando a LGPD: Técnicas de anonimização 46
5. O risco como elemento do sistema normativo de proteção de dados pessoais 55

PARTE II - Privacidade, design e padrões enganosos 72
6. Privacy by Design: uma mudança de mentalidade 73
7. Guia do EDPB sobre padrões obscuros em redes sociais e a crise do consentimento 81

PARTE III - Dados pessoais sensíveis: desafios e discussões 88
8. Explorando a fronteira difusa entre dado pessoal e dado pessoal sensível 89
9. Inferências e Dados de Saúde: o Caso Cryopraxis 100
10. Dados sensíveis e as tecnologias de reconhecimento facial 110
11. Caso Grindr: Requisitos do consentimento e tratamento de dados sensíveis 116

PARTE IV - Inteligência artificial e decisões automatizadas 128
12. Inteligência Artificial: conceito, desafios e tendências regulatórias 129
13. Decisões automatizadas: mapeamento do debate e análise processual 146
14. Regulação da Inteligência Artificial no Brasil 163

PARTE V - Intersecções da proteção de dados 172
15. Quem regula a Internet? 173
16. Regulação de Serviços Digitais na União Europeia: uma análise do DSA 178
17. Metaverso é o futuro da internet? 187
18. Proteção de dados pessoais e concorrência: panorama das principais intersecções 190
19. Proibido para menores de 18 anos: verificação de idade e proteção de dados de crianças e adolescentes 203

PARTE VI - Interpretações de órgãos de *enforcement* 211
20. Estabelecendo parâmetros para o compartilhamento de dados no Poder Público 212
21. Interesse e Legitimidade: a visão da ANPD sobre a base legal do legítimo interesse 228

7

Guia do EDPB sobre padrões obscuros em redes sociais e a crise do consentimento

Anna Bentes
Paula Guedes
Pedro Martins

Lançamento do Guia

O European Data Protection Board (EDPB) lançou no dia 21 de março de 2022o Guia "Padrões obscuros em plataformas de rede social: como reconhecê-los e evitá-los" (*Dark patterns in social media platform interfaces: How to recognise and avoid them*). O guia oferece recomendações práticas para designers e usuários de rede social sobre como acessar e evitar os padrões obscuros que infringem as diretrizes do Regulamento de Proteção de Dados Pessoais (General Data Protection Regulation, GDPR).

O objetivo da publicação é estabelecer orientações para o design das interfaces de plataformas de mídias sociais, de modo a relembrar as obrigações oriundas do GDPR, principalmente os princípios de legalidade, justiça, transparência, limitação de finalidades e minimização já que os padrões obscuros violam claramente tais princípios, apesar de os cumpri-los formalmente. Além disso, o guia visa ampliar a conscientização dos usuários sobre seus direitos e os riscos vindos desses padrões.

Dark patterns

Afinal, o que são esses **padrões obscuros**? O termo **"padrões obscuros" (dark patterns)** foi criado pela UX designer **Harry Brignull** em 2010 para designar "truques usados em sites e aplicativos para levá-lo a fazer coisas que você não queria" em benefício do negócio em

questão. No âmbito do guia, os padrões obscuros são considerados os recursos da interface e da experiência de usuário em redes sociais que induzem os usuários a tomarem decisões não intencionais que podem ser potencialmente danosas, especialmente, em relação ao processamento de seus dados pessoais. Em outras palavras, esses padrões visam influenciar o comportamento do usuário, de forma a prejudicar sua capacidade de proteger efetivamente seus dados pessoais e a fazer escolhas conscientes. Os padrões obscuros não necessariamente levam à violação da regulação de proteção de dados, por vezes, podem ficar na fronteira entre o legal e o ilegal[50] ou podem levar também à violação das regulações de proteção ao consumidor.

Principais pontos do guia da EDPB

Em um contexto de ambientes cada vez mais personalizados, a EDPB chama atenção que, embora essas tendências possam aumentar a facilidade de uso dos serviços digitais, muitos desses recursos de interface e formas de experiência do usuário podem ser usados para promover comportamentos que vão contra o espírito e os princípios do GDPR. Ressalta-se, ainda, que os padrões obscuros são especialmente relevantes no contexto da economia da atenção[51], no qual a atenção dos usuários é considerada uma *commodity* e, portanto, esses truques podem ser ferramentas estratégicas para distrair os usuários de formas de proteção dos seus dados e da sua privacidade.

O guia se volta basicamente para os controladores de interfaces de usuários gráficas (computadores e smartphones), apresentando um panorama detalhado com diferentes exemplos dos padrões obscuros em mídias sociais estruturados em torno de duas categorias: **1. Padrões baseados em conteúdo**: envolvem os conteúdos como a redação textual, o tom e o contexto das frases e os componentes da informação; **2. Padrões baseados em interface**: estão ligados aos modos de exibir os conteúdos, navegar e interagir na plataforma. Além disso, o documento oferece exemplos de padrões obscuros em diferentes momentos do uso de dados em redes sociais: a inscrição e registro do usuário quando entra na plataforma; as formas de notificação sobre o controle da privacidade; gerenciamento do consentimento; exercício dos direitos do titular no uso dos serviços; e, por fim, quando decidem encerrar suas contas.

---

50 How Dark Patterns Trick You Online: **https://www.youtube.com/watch?v=kxkrdLI6e6M**.

51 Ver mais em: BENTES, Anna. Quase um tique: economia da atenção, vigilância e espetáculo em uma rede social. Rio de Janeiro: Editora UFRJ, 2021.

Sobre as interfaces das redes sociais, o guia chama atenção para 6 principais categorias[52] padrões obscuros que podem comprometer sua capacidade de tomar decisões informadas:

1. **Sobrecarga** (*Overloading*): meios de bombardear o usuários com várias informações e conteúdos, visando confundi-lo para aceitar compartilhar mais dados sem a sua intenção, como em repetidas solicitações para que o usuário forneça mais dados pessoais do que o necessário ou para que concordem com outras finalidades de processamento (*continuous prompting*); quando os usuários querem obter certas informações, realizar operação de controle ou exercer algum direito e é particularmente difícil, pois precisam navegar por muitas páginas (*privacy maze*); ou quando é apresentado ao usuário muitas opções, fazendo-os ignorar ou perder configurações de proteção de dados (*too many options*)

2. **Deixando passar** (*Skipping*): formas de fazer o usuário esquecer ou não pensar sobre aspectos de proteção de dados, por exemplo, quando os recursos mais invasivos de dados estão ativos por padrão (*deceptive snugness*); ou quando informações sobre proteção de dados concorrem com outros elementos na interface, distraindo os usuários (*look over there*).

3. **Agitação** (*Stirring*): meios de apelo a aspectos emocionais ou uso de *nudges*[53] visuais, por exemplo, utilizando textos ou elementos visuais como forma de convencer os usuários a se sentirem seguros ou culpados, influenciando seu estado emocional para que eles tomem decisões que vão contra a garantia de seus direitos de proteção de dados (*emotional steering*); ou quando são usados estilos visuais em infor-

52 No anexo do Guia, o documento apresenta uma relação entre as categorias listadas por ele e sua relação com outros tipos de padrões obscuros, bem como quais preocupações eles levantam em relação aos princípios do GDPR.

53 *Nudges* são elementos do contexto no qual usuários tomam decisões que funcionam como "empurrões" ou "cutucões" para estimular o usuário a tomar certa decisão ou realizar determinado comportamento.

mações ou formas de controle de dados que empurre o usuário a formas menos restritas e invasivas de privacidade (*hidden in plain sight*).

4. **Obstruindo** (*Hindering*): formas de bloqueio ou obstrução nas formas de informar ou manejar os dados ao tornar a ação o mais difícil possível, como quando os usuários não encontram links em funcionamento para informações adicionais a respeito do processo que desejam praticar, seja registro, revogação do consentimento ou exercício de direitos (*dead end*); quando processos exigem mais etapas do que o necessário (*longer than necessary*); ou quando é fornecida informação enganosa (*misleading information*);

5. **Inconstante** (*Fickle*): meios de tornar a interface inconsistente e obscura, tornando difícil o usuário navegar em ferramentas de proteção de dados para entender os propósitos do processamento, por exemplo, quando informações sobre proteção de dados aparecem em diferentes locais e formas ou em linguagem de difícil entendimento, confundindo o usuário (*lacking hierarchy*); ou quando esta informação está fora de contexto, de forma a dificultar o seu encontro pelo usuário (*decontextualising*)

6. **Deixado no escuro** (*Left in the dark*): formas da interface de esconder informações ou ferramentas de proteção e controle dos dados, ou deixar os usuários sem informações sobre como seus dados são processados e qual controle eles têm de exercitar seus direitos, exemplo disso é quando certos sites deixam de oferecer determinada língua em uma de suas páginas (*language discontinuity*), quando são fornecidas informações conflitantes (*conflicting information*); ou quando são utilizadas palavras ou expressões ambíguas ou vagas (*ambiguous wording or information*)

À vista disso, o EDPB ressalta a importância do princípio do tratamento justo (nº 1, alínea a do art. 5º do GDPR) - que pode ser comparado ao princípio da boa-fé no direito brasi-

leiro - para a avaliação da existência de padrões obscuros. Isso porque a equidade exige que os dados pessoais dos usuários não sejam tratados de forma prejudicial, discriminatória, inesperada ou enganosa para os titulares de dados. Por isso, se a interface tiver informações insuficientes ou enganosas, por exemplo, pode ser classificada como uma forma de padrão obscuro e, assim, classificada como tratamento injusto.
Porém, para além da justiça, o guia ressalta também a importância dos princípios da responsabilidade/prestação de contas (*accountability*) e transparência, além das obrigações relacionadas à proteção de dados *by design*, requisitos de bases legais e cumprimento dos direitos dos titulares de dados pessoais. No que tange à noção de proteção de dados by design e by default, o EDPB relembra a **orientação 4/2019 (Guidelines 4/2019 on Article 25 Data Protection by Design and by Default)** que listou os principais elementos para sua concretização na prática: autonomia, interação, expectativa, escolha do consumidor, ausência de engano, equilíbrio de poder e confiança.

Por fim, o EDPB listou também algumas recomendações e melhores práticas que facilitam a implementação efetiva do GDPR pelos controladores de interfaces de mídias sociais. Dentre elas, podemos citar:

i. disponibilização de atalhos (shortcuts) - links para informações, ações ou configurações para auxiliar usuários a gerenciar seus dados;
ii. disponibilização de informações de forma clara em locais que o usuário espera encontrar;
iii. identificação da identidade da autoridade de supervisão de proteção de dados;
iv. disponibilização de política de privacidade de forma destacada e granular;
v. possibilidade de comparar mudanças nas políticas de privacidade;
vi. utilização de redação coerente;
vii. fornecimento de definições em linguagem simples;
viii. utilização de elementos visualmente impactantes nas interfaces quando o tópico relacionar-se à proteção de dados;
ix. integração da experiência do usuário com elementos e conceitos de proteção de dados;
x. utilização de exemplos, sempre que possível.

Por muitos anos, diferentes controladores utilizaram-se de variadas estratégias, incluindo o uso de padrões obscuros, para garantir um cumprimento meramente formal dos regramentos de proteção de dados, de modo a não garantir a proteção efetiva dos titulares de dados na prática. Um ponto especialmente relevante desse cumprimento meramente

formal pode ser identificado no uso indiscriminado do consentimento como base legal para o tratamento de dados.

Análise

Pode-se dizer que há um movimento de "banalização" do consentimento, valendo-se de aceites genéricos ou que não podem ser negados pelo titular para legitimar atividades de tratamento de dados. Esse movimento foi denominado por alguns autores como "**crise do consentimento**", que descreve a dessensibilização do consentimento pelo titular ao ser constantemente requerido para consentir com determinada atividade de tratamento.

Como resposta a essa tendência, autoridades de proteção de dados e legisladores começam a adotar uma postura mais rígida. O guia adotado pelo EDPB evidencia o atual movimento regulatório das autoridades, principalmente de proteção de dados pessoais, contra a tendência de utilização de padrões obscuros em interfaces de mídias sociais tanto para evitar o compartilhamento indevido de dados quanto a aquisição do consentimento entre outros possíveis danos aos usuários

Ainda em 2019, o Tribunal de Justiça da União Europeia **julgou o caso "Planet49"**, em que se analisou o que constituía um consentimento livre. **O Tribunal determinou que** o consentimento livre deve ser entendido como "um comportamento ativo com uma visão clara" e o mero uso do serviço não constitui um consentimento livre. Ainda, checkboxes "pré marcados" também violam a ideia de consentimento livre, e finalidades diferentes requerem pedidos de consentimento diferentes.

Já no início de 2022, o CNIL (Autoridade de Proteção de Dados da França), multou o **Google** e **Facebook** em 150 e 60 milhões de euros, respectivamente, por não oferecerem em suas plataformas uma maneira igualmente fácil de recusar a coleta de cookies quanto é para aceitá-los.

Por fim, talvez o caso de maior impacto seja o **Caso IAB (Interactive Advertising Bureau), julgado pela Autoridade Belga de Proteção de Dados**, em que se declarou ilegal o Transparency & Consent Framework disponibilizado pelo IAB Europe, visto que, dentre outros fatores, o consentimento coletado não atendia aos requisitos da GDPR.

O movimento de banimento ou drástica restrição dessas práticas não está presente

apenas no continente europeu, mas mundialmente. Por exemplo, a Lei de Privacidade Consumidor da Califórnia (CCPA) de 2018 foi **atualizada em 2021 para proibir padrões obscuros que têm o efeito substancial de subverter ou prejudicar a escolha do consumidor de optar por não participar de esquemas em que seus dados pessoais estão sendo vendidos**[54].

54 VINCENT, James. California bans 'dark patterns' that trick users into giving away their personal data. The Verge, publicado em 16 mar. Disponível em: **https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data**. Acesso em 23 mar. 2022.